أمن المعلومات

GS224-6

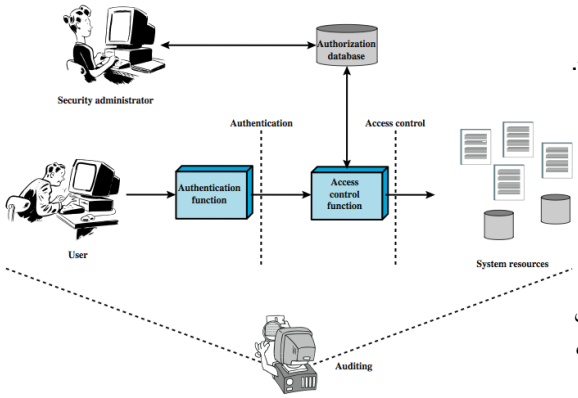
التحكم في الوصول

يمكننا أن ننظر إلى التحكم في الوصول كعنصر مركزي لأمن الحاسبات ، تحدد التوصية (ITU-T/X.800) التحكم في الوصول: **"منع الاستخدام غير المصرح به لمورد ما ، بما في ذلك منع استخدام المورد بطريقة غير مصرح بها"**

- الأهداف
  - منع المستخدمين غير المصرح لهم من الوصول إلى الموارد
  - منع المستخدمين الشرعيين من الوصول إلى الموارد بطريقة غير مصرح بها
  - وتمكين المستخدمين الشرعيين من الوصول إلى الموارد بطريقة مصرح بها
  - الأخذ في الاعتبار المجموعات و المستخدمين القادرين على المصادقة على نظام ثم يتم تعيين حقوق الوصول إلى موارد معينة على النظام.

مبادئ التحكم في الوصول

نتعامل هنا مع مفهوم أضيق وأكثر تحديدًا للتحكم في الوصول، والذي ينفذ سياسة أمنية تحدد من أو ما الذي يمكنه الوصول إليه من موارد نظام محدد، ونوع الوصول المسموح به في كل حالة.
يوضح الشكل المفهوم الأوسع للتحكم في الوصول. فبالإضافة إلى التحكم في الوصول ، يشمل هذا المفهوم الأوسع الكيانات والوظائف التالية:



المصادقة: التحقق من هوية المستخدم والمطالب بها من قبل النظام أو لصالحه.
التفويض: منح حق أو إذن لكيان النظام للوصول إلى موارد النظام. تحدد هذه الوظيفة من يمكن الوثوق به لغرض معين.
التدقيق: مراجعة وفحص مستقلين لسجلات وأنشطة النظام من أجل اختبار مدى كفاية ضوابط النظام ، ولضمان الامتثال للسياسة المعمول بها وإجراءات التشغيل ، واكتشاف الانتهاكات الأمنية ، والتوصية بأي تغييرات مشار إليها في الضوابط والسياسات و إجراءات.

مبادئ التحكم في الوصول

تتوسط آلية التحكم في الوصول بين المستخدم (أو عملية يتم تنفيذها نيابة عن المستخدم) وموارد النظام ، مثل الملفات وقاعدة البيانات. يجب أن يقوم النظام أولاً بالمصادقة على المستخدم الذي يسعى للوصول. بعد ذلك ، تحدد وظيفة التحكم في الوصول ما إذا كان الوصول المطلوب المحدد من قبل هذا المستخدم مسموحًا به ام لا.

يحتفظ مسؤول الأمان بقاعدة بيانات التفويضات التي تحدد نوع الوصول إلى الموارد المسموح بها لهذا المستخدم. تستشير وظيفة التحكم في الوصول قاعدة البيانات هذه لتحديد ما إذا كان سيتم منح الوصول أم لا. تراقب وظيفة التدقيق وتحتفظ أيضا بسجل لوصول المستخدم إلى موارد النظام.

تحتوي جميع أنظمة التشغيل على عنصر تحكم في الوصول بدائي (على الأقل)، وفي بعض الحالات قوي جدًا. تتضمن أيضًا تطبيقات أو أدوات مساعدة معينة ، مثل نظام إدارة قاعدة البيانات ، وفرض وظائف التحكم في الوصول.

سياسات التحكم في الوصول

- **التحكم في الوصول التقديري** (Discretionary access control (DAC)): استنادًا إلى هوية مقدم الطلب وقواعد الوصول
- **التحكم في الوصول الإلزامي** (Mandatory access control (MAC)): استنادًا إلى مقارنة وسم الأمان مع التصاريح الأمنية (إلزامي: لا يمكن لمن لديه حق الوصول إلى مورد ما أن يمرره إلى الآخرين)
- **التحكم في الوصول المستند إلى الدور** (Role-based access control (RBAC)): استنادًا إلى أدوار المستخدم
- **التحكم في الوصول المعتمد على السمات** (Attribute-based access control (ABAC)): استنادًا إلى سمات المستخدم والموارد والبيئة الحالية

متطلبات التحكم في الوصول

- **مدخلات موثوقة**: آلية للمصادقة - تفترض أن المستخدم تم التحقق منه؛ وبالتالي، هناك حاجة إلى آلية المصادقة كواجهة أمامية لنظام التحكم في الوصول. يجب أن تكون المدخلات الأخرى لنظام التحكم في الوصول موثوقة أيضًا.
- **المواصفات الدقيقة والخشنة**: تنظيم الوصول على مستويات مختلفة بحيث تسمح المواصفات الدقيقة بالوصول المنظم على مستوى الحقول / السجلات الفردية في الملفات (أوسمة أو قاعدة بيانات كاملة) ؛ ووصول منفرد من قبل مستخدم بدلاً من وصول متسلسل. يجب أن يكون مسؤولو النظام أيضًا قادرين على اختيار مواصفات خشنة لبعض الفئات للوصول إلى الموارد.
- **الامتياز الأقل**: الحد الأدنى من الإذن للقيام بالعمل ، بحيث يتم منح كل كيان في نظام الحد الأدنى من موارد النظام والتراخيص اللازمة للقيام بعمله. يميل هذا المبدأ إلى الحد من الضرر الذي يمكن أن ينجم عن حادث أو خطأ أو عمل غير مصرح به.

متطلبات التحكم في الوصول

- **فصل المهام**: يجب تقسيم الخطوات في وظيفة ما للنظام بين أفراد مختلفين ، وذلك لمنع فرد واحد من تخريب العملية.
- **السياسات المفتوحة والمغلقة:** تسمح السياسة المغلقة بالوصول فقط للمصرح به على وجه التحديد ؛ تسمح السياسة المفتوحة لجميع عمليات الوصول باستثناء تلك المحظورة صراحة.
- **مجموعة السياسات وحل التعارضات**: قد تطبق سياسات متعددة على فئة معينة من الموارد ، وتحتاج إلى إجراء لحل التعارض بين هذه السياسات.
- **السياسات الإدارية**: تحديد من يمكنه إضافة قواعد التفويض أو حذفها أو تعديلها ، ويحتاج إلى التحكم في الوصول وآليات التحكم الأخرى لفرض هذه السياسات الإدارية.

عناصر التحكم في الوصول

- **المستخدم** (Subject): هو الكيان القادر على الوصول إلى المكونات/كائنات، وعادة ما يكون عملية.
  - يحصل أي مستخدم أو تطبيق فعليًا على حق الوصول إلى كائن عن طريق عملية تمثله. عادة ما يكون المستخدم مسؤولاً عن الإجراءات التي بدأها ، ويمكن استخدام خيارات التدقيق لربط المستخدم واجراءات الامن التي ذات العلاقة التي تم تنفيذها على كائن ما.
  - تحدد أنظمة التحكم في الوصول الأساسية (عادة) ثلاث فئات من المستخدمين:
    - **المالك**: قد يكون هو منشئ المورد، مثل ملف. بالنسبة لموارد النظام، قد تكون الملكية إلى مسؤول النظام. بالنسبة لموارد مشروع ، قد يتم تكون الملكية إلى مسؤول المشروع أو المدير.
    - **المجموعة**: بالإضافة إلى الامتيازات المعينة للمالك ، يمكن أيضًا منح مجموعة محددة من المستخدمين حقوق الوصول ، بحيث تكون العضوية في المجموعة كافية لممارسة حقوق الوصول هذه.
    - **العالم**: يتم منح أقل قدر من الوصول للمستخدمين القادرين على الوصول إلى النظام ولكن لم يتم تضمينهم في فئات المالك والمجموعة لهذا المورد.

عناصر التحكم في الوصول

- **الكائن** (Object) : هو أي مورد يتم التحكم في الوصول إليه. بشكل عام ، الكائن هو كيان يستخدم لاحتواء و/ أو تلقي المعلومات.
  - على سبيل المثال السجلات والقوالب والصفحات والمقاطع والملفات وأجزاء من الملفات والأدلة وتفرعات الادلة وصناديق البريد والرسائل والبرامج.
  - يعتمد عدد وأنواع الكائنات التي يجب حمايتها بواسطة نظام التحكم في الوصول على البيئة التي يتم فيها التحكم في الوصول.
- **حق الوصول** (Access Right) : يصف حق الوصول الطريقة التي يمكن للمستخدم من خلالها الوصول إلى الكائن. يمكن أن تشمل حقوق الوصول ما يلي: قراءة ، كتابة ، تنفيذ ، حذف ، إنشاء ، بحث.

التحكم في الوصول التقديري ((DAC))

للتحكم في الوصول التقديري ، تتمثل الطريقة العامة للتحكم في الوصول كما ينفذها نظام التشغيل أو نظام إدارة قاعدة البيانات في **مصفوفة الوصول**.

- غالبًا ما تكون على شكل مصفوفة وصول ، احد ابعاد المصفوفة توجد بها المستخدمين (الصفوف) ، وتوجد الكائنات في البعد الآخر (الأعمدة). تحدد كل خلية حقوق وصول المستخدم المحددة لهذا الكائن. مصفوفة الوصول يمكن تقسيمها/تحليلها عن طريق أي صف أو عمود
- **البعد الأول** للمصفوفة يتكون من المستخدمين المحددة التي قد تحاول الوصول إلى البيانات. عادةً ما تتكون هذه القائمة من مستخدمين فرديين أو مجموعات مستخدمين ، على الرغم من إمكانية التحكم في الوصول للأجهزة الطرفية أو الأجهزة المضيفة أو التطبيقات بدلاً من المستخدمين أو بالإضافة إليهم.

التحكم في الوصول التقديري ((DAC))

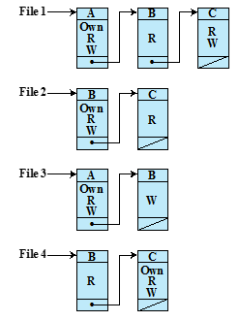
- **البعد الثاني** يتكون من الكائنات التي يمكن الوصول إليها. في أعلى مستوى من التفاصيل ، قد تكون الكائنات عبارة حقول بيانات فردية. وقد تكون عبارة عن مجموعات مجمعة ، مثل السجلات أو الملفات أو حتى قاعدة البيانات بأكملها ، أو كائنات في المصفوفة. تشير كل خلية في المصفوفة إلى حقوق الوصول لهذا المستخدم على هذا الكائن. من الناحية العملية ، مصفوفة الوصول يمكن انجازها عن طريق تقسيمها بإحدى طريقتين ، كما سيتم عرضه تاليا.

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

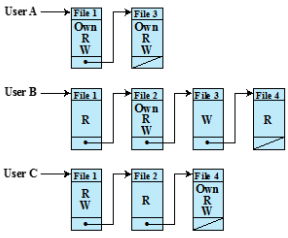
(a) Access matrix

بنية بيانات التحكم في الوصول

- قوائم التحكم في الوصول (موزعة حسب العمود)
- تذاكر القدرات (موزعة حسب الصف)
- لاحظ أيضًا التمثيل البديل لجدول التفويضات



(b) Access control lists for files of part (a)



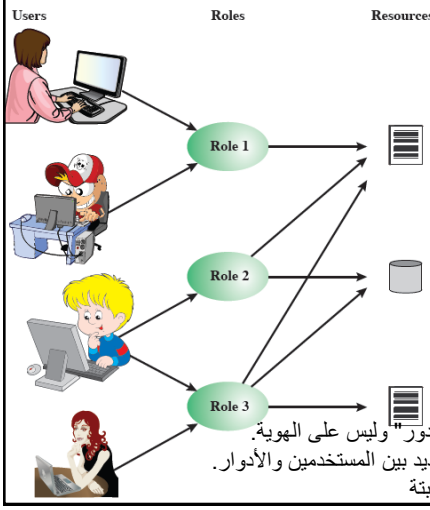
(c) Capability lists for files of part (a)

التمثيل البديل لجدول التفويضات

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

التحكم في الوصول المستند إلى الدور

تحدد أنظمة التحكم في الوصول التقديري (DAC) التقليدية حقوق الوصول للمستخدمين فرادى ومجموعات المستخدمين. في المقابل ، يعتمد نظام التحكم في الوصول المستند إلى الدور (RBAC) على الأدوار المفترضة للمستخدمين على النظام بدلاً من هوية المستخدم.



عادة ، تحدد نماذج نظام التحكم في الوصول المستند إلى الدور (RBAC) الدور كمهمة وظيفية داخل المؤسسة. تقوم أنظمة (RBAC) بتعيين حقوق الوصول إلى الأدوار بدلاً من المستخدمين الفرديين. في المقابل ، يتم تعيين أدوار مختلفة المستخدمين ، إما بشكل ثابت أو ديناميكي ، وفقًا لمسؤولياتهم. يتمتع (RBAC) الآن باستخدام تجاري واسع النطاق ولايزال مجال نشط للبحث .

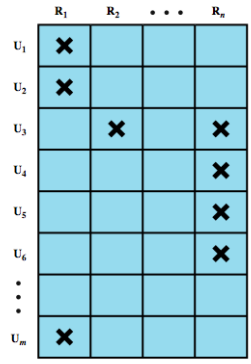
الوصول على أساس "الدور" وليس على الهوية.
علاقة عديد – الى – عديد بين المستخدمين والأدوار.
الأدوار غالبًا ما تكون ثابتة

التحكم في الوصول المستند إلى الدور

- **علاقة المستخدمين بالأدوار هي على شكل عديد – الى – عديد** ، كما هو الحال بالنسبة لعلاقة الأدوار بالموارد ، أو كائنات النظام ، كما هو موضح في الشكل السابق.
- **تتغير مجموعة المستخدمين** في بعض البيئات بشكل متكرر ، وقد يتم تحديد دور واحد أو أكثر لمستخدم ما ديناميكيًا.
- في معظم البيئات غالبا ما يكون **تحديد الأدوار في النظام ثابتا** ، مع عمليات إضافة أو حذف عرضية فقط.
- **يكون لكل دور حقوق وصول محددة إلى مورد واحد أو أكثر**. كذلك ، الموارد وحقوق الوصول الخاصة المرتبطة بدور معين غالبا ما تتغير بشكل غير متكرر.

التحكم في الوصول المستند إلى الدور

يمكننا استخدام تمثيل مصفوفة الوصول لتوضيح العناصر الرئيسية لنظام (RBAC) بعبارات بسيطة ، كما هو موضح في الشكل. المصفوفة العليا تربط المستخدمين الفرديين بالأدوار. عادةً ما يكون عدد المستخدمين أكثر من عدد الأدوار. كل خلية في المصفوفة تكون إما فارغة أو محددة ، وتشير الأخيرة إلى أن هذا المستخدم قد تم تعيينه لهذا الدور.



مصفوفة المستخدمين-الأدوار والأدوار-الكيانات

OBJECTS

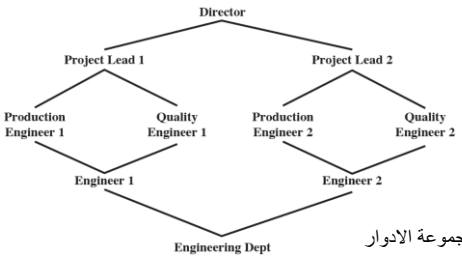
ROLES	R1	R2	Rn	F1	F1	P1	P2	D1	D2
R1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R2		control		write *	execute			owner	seek *
Rn			control		write	stop			

التحكم في الوصول المستند إلى الدور

- قد يتم تعيين أدوار متعددة لمستخدم واحد (أكثر من علامة واحدة في صف واحد) وأنه قد يتم تعيين عدة مستخدمين لدور واحد (أكثر من علامة واحدة في عمود). المصفوفة السفلية لها نفس بنية مصفوفة التحكم في الوصول إلى (DAC) مع تمثيل الأدوار كمستخدمين . عادة ، هناك عدد قليل من الأدوار والعديد من الكائنات أو الموارد. في هذه المصفوفة ، مدخلات الخلية هي حقوق الوصول المحددة التي تتمتع بها الأدوار. لاحظ أنه يمكن معاملة الدور ككائن ، مما يسمح بتعريف التدرجات الهرمية للدور.
- (RBAC) يفسح المجال للتنفيذ الفعال لمبدأ الامتياز الأقل، حيث يحتوي كل دور على الحد الأدنى من مجموعة حقوق الوصول اللازمة لهذا الدور. يتم تعيين مستخدم لدور يمكّنه من أداء ما هو مطلوب فقط حسب الدور. العديد من المستخدمين المعينين لنفس الدور يتمتعون بنفس الحد الأدنى من مجموعة حقوق الوصول.

التحكم في الوصول المستند إلى الدور :- خصائص

- مكونات مخطط نظام (RBAC)
  - المستخدم: الشخص الذي يمكنه الوصول إلى نظام الحاسب وله معرف مرتبط به.
  - الدور: مهمة وظيفية محددة داخل المؤسسة تتحكم في نظام الحاسب. عادة ما يرتبط كل دور بوصف للسلطة والمسؤولية الممنوحة لهذا الدور والمستخدم الذى يتولى هذا الدور.
  - الأذن: الموافقة على وضع معين للوصول إلى كائن واحد أو أكثر. (حق الوصول، الامتياز، الترخيص).
  - الجلسة: ربط ما بين المستخدم ومجموعة فرعية نشطة من مجموعة الأدوار التي تم تعيينها إليه.
- التسلسل الهرمي للأدوار
  - المدير لديه معظم الامتيازات
  - يرث كل دور جميع الامتيازات من الأدوار الأدنى
  - يمكن أن يرث الدور من أدوار متعددة
  - يمكن تعيين امتيازات إضافية للدور



- شروط (قيود) الواجبة على الأدوار أو ما بين الأدوار
  - لا تعتمد على بعض
    - تنظم الأدوار بحيث يكون للمستخدم دور واحد فقط في مجموعة الادوار
    - يمنح الأذن لدور واحد فقط في المجموعة
- العلاقة الأساسية: تعيين العدد الأقصى (من المستخدمين) يمكن تعيينه لدور معين (على سبيل المثال ، دور رئيس قسم)
- الاسبقية: لا يمكن تعيين دور للمستخدم إلا إذا تم تعيينه فعلا لدور آخر مسبقا.

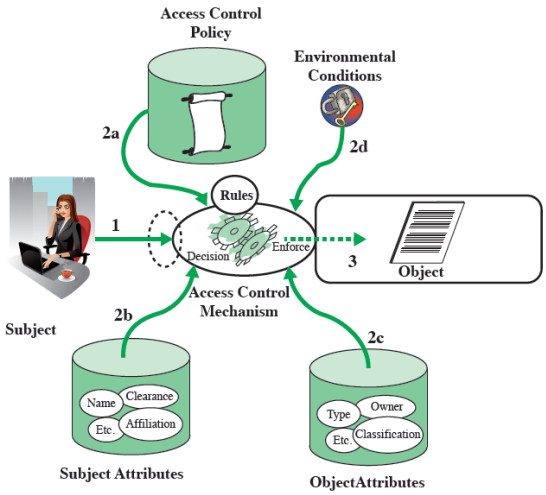
التحكم في الوصول المستند إلى السمات

- حديث
- تعريف التراخيص/الامتيازات التي تبين حالات خصائص كل من المورد والمستخدم
  - على سبيل المثال: اذا كان لكل مورد سمة تحدد المستخدم الذى انشئه، اذن، يمكن لقاعدة وصول واحدة ان تحدد امتيازات الملكية للمنشئين
- القوة: مرونتها وقوتها التعبيرية
- اهتمام كبير بتطبيق هذا النموذج على الخدمات السحابية

أنواع السمات

- **سمات المستخدم**
  - المستخدم هو كيان نشط يتسبب في تدفق المعلومات بين الكائنات أو يغير حالة النظام
  - تحدد السمات هوية وخصائص المستخدم (مثل: المعرف والمنظمة والمسمى الوظيفي)
- **سمات الكائن**
  - الكائن (أو المورد) هو كيان مرتبط بنظام المعلومات بشكل سلبي (متقبل للطلبات) يحتوي على معلومات أو يستقبلها (أجهزة، ملفات، سجلات، جداول، عمليات، برامج، ...)
  - تملك الكائنات سمات يمكن الاستفادة منها لاتخاذ قرارات التحكم في الوصول (العنوان ، الموضوع ، المؤلف ، التاريخ)
- **سمات البيئة**
  - وصف البيئة التشغيلية والتقنية وحتى الظرفية أو السياق الذي يحدث فيه الوصول إلى المعلومات (التاريخ الحالي ، النشاط الحالي للفيروسات/المتسللين ، مستوى أمان الشبكة).
  - لا ترتبط بالمورد أو المستخدم ولكن ربما لها علاقة بالسياسات الأمنية المتبعة.
  - تم تجاهل هذه السمات إلى حد كبير حتى الآن في معظم سياسات التحكم في الوصول

نموذج لسيناريو (ABAC)



- نظام (ABAC) هو نموذج منطقي للتحكم في الوصول متميز لأنه يتحكم في الوصول إلى الكائنات من خلال تقييم القواعد مقابل سمات الكيانات (المستخدم والكائن) ، والعمليات ، والبيئة ذات الصلة بالطلب. يعتمد (ABAC) على تقييم سمات المستخدم ، وسمات الكائن ، والعلاقة الرسمية أو قاعدة التحكم في الوصول التي تحدد العمليات المسموح بها لمزيج سمات كائن و سمات المستخدم في بيئة معينة.
- يوضح الشكل المكونات الأساسية لنظام (ABAC) وصول المستخدم إلى كائن يتم وفقًا للخطوات التالية:

نموذج لسيناريو (ABAC)

1. مستخدم يطلب الوصول إلى كائن. يتم توجيه هذا الطلب إلى آلية التحكم في الوصول.
2. تخضع آلية التحكم في الوصول لمجموعة من القواعد (2a) التي تم تحديدها من قبل سياسة التحكم في الوصول مسبقة الاعداد. بناءً على هذه القواعد ، تقوم آلية التحكم في الوصول بتقييم سمات المستخدم (2b) والكائن (2c) والظروف البيئية الحالية (2d) لتحديد التفويض.
3. آلية التحكم في الوصول تمنح المستخدم حق الوصول إلى الكائن إذا كان مسموحًا له بالوصول ويرفض الوصول إذا لم يكن مصرحًا له.

يتضح من البنية المنطقية أن هناك أربعة مصادر مستقلة للمعلومات المستخدمة في قرار التحكم في الوصول. يمكن لمصمم النظام تحديد السمات المهمة للتحكم في الوصول فيما يتعلق بالمستخدم والكائنات والظروف البيئية. يمكن لمصمم النظام أو أي سلطة أخرى ان يحدد سياسات التحكم في الوصول ، على شكل قواعد لأي مجموعة مرغوبة من سمات المستخدم، والكائن ، والظروف البيئية ، مما يؤكد أن هذا النهج قوي ومرن. ومع ذلك ، فإن التكلفة من حيث تعقيد التصميم والتنفيذ ومن حيث تأثير الأداء ، فمن المرجح أن تتجاوز تكلفة طرق التحكم في الوصول الأخرى ، وهذه مقايضة يجب أن تقوم بها سلطة النظام.